Blockchain a prawo

Jacek Czarnecki

nowe technologie
nowe rozwiązania płatnicze
WARDYŃSKI I WSPÓLNICY
czerwiec 2015

Bitcoin otworzył spektrum możliwości oraz prawniczą puszkę Pandory. Jeszcze większy potencjał i kolejne wyzwania prawne niesie technologia u podstaw Bitcoina, czyli blockchain.

Koncepcja waluty cyfrowej Bitcoin powstała w 2008 r., a dziś jest jednym z najgoręcej dyskutowanych tematów w debatach o przyszłości systemu finansowego. Innowacyjny ładunek Bitcoina opiera się przede wszystkim na decentralizacji tej waluty. W przypadku Bitcoina nie istnieje centralny emitent oraz – podobnie jak w przypadku gotówki, a w przeciwieństwie do pieniądza bezgotówkowego – przepływ płatności nie wymaga pośrednictwa zaufanej trzeciej strony, takiej jak bank. Transakcje potwierdzane są poprzez szczególnego rodzaju konsensus, osiągany w drodze głosowania przez użytkowników sieci Bitcoin nazywanych minerami (górnikami), przy czym wartość „głosu" zależy od mocy obliczeniowej dostarczonej przez danego minera na potrzeby potwierdzania transakcji. Inne cechy Bitcoina, takie jak względna anonimowość transakcji czy niskie (choć istniejące) koszty transakcyjne, są pochodnymi decentralizacji tej cyfrowej waluty.

To właśnie decentralizacja Bitcoina, połączona z cyfrową naturą tej waluty, powoduje największe problemy prawne i podatkowe związane z jego kreacją i obrotem (opisywaliśmy je w raporcie „Wirtualne waluty", dostępnym do pobrania tutaj). Brak emitenta i pośredników, anonimowość uczestników transakcji oraz zdecentralizowany system rozliczania transakcji sprawiają, że do Bitcoina trudno zastosować tradycyjne instytucje prawne.

Bitcoin 2.0

Bitcoin jest przede wszystkim protokołem komunikacyjnym, czyli zbiorem zasad wymiany informacji pomiędzy urządzeniami. Protokół Bitcoina dodatkowo wykorzystuje zaawansowaną kryptografię, tak aby zapewnić bezpieczeństwo sieci. Komunikujące się z użyciem tego protokołu komputery wytwarzają bazę danych, która w przypadku Bitcoina stanowi księgę (rejestr) wszystkich wykonanych transakcji.

Taki rejestr przechowywany jest na różnych komputerach i serwerach na całym świecie, nazywanych węzłami sieci Bitcoin. Baza danych utrzymywana przez węzły nazywana jest *blockchainem* („łańcuchem bloków"), gdyż przyjmuje formę najdłuższego możliwego ciągu bloków, czyli plików zawierających zapis grupy transakcji. *Blockchain* jest bazą zdecentralizowaną, ponieważ nie jest prowadzony przez jeden centralny podmiot, ale jednocześnie przez tysiące węzłów sieci Bitcoin. Architektura protokołu Bitcoin zapewnia, że większość węzłów w sieci z ogromnym prawdopodobieństwem będzie utrzymywać identyczną bazę danych. Ta spójność zapewniana jest w drodze wcześniej wspomnianego konsensusu uczestników sieci.

Wraz z rozpowszechnianiem się protokołu Bitcoina i rozrastaniem się *blockchaina* pojawiły się pomysły zastosowania tej bazy danych do innych celów niż przechowywanie zapisów transakcji.

Takim pomysłem jest usługa *Proof of existence*, która umożliwia zamieszczenie w łańcuchu bloków kryptograficznej informacji o wybranym przez użytkownika dokumencie wraz z umieszczeniem znacznika czasu. Sam dokument nie jest udostępniany, ale wykorzystanie osiągnięć kryptografii pozwala na sprawdzenie z całkowitą pewnością, czy dokument nie był modyfikowany po jego umieszczeniu w *blockchainie*. Ze względu na decentralizację łańcucha bloków nie ma również możliwości ingerencji w zamieszczoną w nim informację o dokumencie. *Proof of existence* oraz matematyczne podstawy działania tej usługi mogą być w przyszłości z powodzeniem wykorzystane przez sądy w celu przeprowadzenia dowodu z dokumentu. Tego typu usługi oparte na *blockchainie* stanowią bowiem w odniesieniu do danych cyfrowych pewien odpowiednik notarialnego potwierdzenia istnienia dokumentu tradycyjnego, z tym że mamy tu do czynienia z pewnością gwarantowaną przez zasady matematyki.

Zdecentralizowana wymiana wartości

Inne pomysły na wykorzystanie *blockchaina* polegają na przyjęciu, że zapisy (salda) w rejestrze transakcji, jakim jest łańcuch bloków, miałyby oznaczać nie walutę, ale inne nośniki wartości. Skoro Bitcoin jest walutą opartą na łańcuchu bloków, inne łańcuchy mogą służyć na przykład jako rejestry akcji lub udziałów w spółkach. Podobnie jak Bitcoin jest walutą funkcjonującą bez potrzeby istnienia banku centralnego, obrót jednostkami udziałowymi opartymi na technologii *blockchaina* mógłby odbywać się całkowicie bez pośrednictwa giełdy, bez większych kosztów i innych uczestników tradycyjnych transakcji oraz niemalże w czasie rzeczywistym. Takie rozwiązania wprowadza już amerykański Nasdaq.

Bardziej dalekosiężne plany obejmują przyznanie jednostkom w łańcuchach bloków roli tokenów reprezentujących inne prawa czy wartości majątkowe. Potencjalnie mogłoby to zrewolucjonizować nasz obecny sposób myślenia o sposobach przenoszenia własności

czy rejestrach publicznych – oparte na *blockchainie* tokeny mogłyby bowiem inkorporować prawa własności nieruchomości czy prawa własności intelektualnej.

Powyższe przykłady pokazują jeden z głównych walorów technologii łańcucha bloków – sposób na decentralizację wymiany wartości. Zgodnie z często przytaczanym przykładem, podobnie jak internet umożliwił zdecentralizowaną wymianę informacji, *blockchain* zrobi to samo w odniesieniu do wartości. Bitcoin zaś jest jedynie pierwszym etapem w rozwoju tej technologii, w którym zastosowano najpopularniejszy środek wymiany wartości między ludźmi – pieniądz.

Co na to prawo?

W krótkim czasie systemy prawne będą musiały odpowiedzieć na wyzwania, które niesie technologia łańcucha bloków. Dość prawdopodobne, że w pierwszej kolejności konieczność ta dotknie regulacji rynków finansowych. Już dziś technologie zbliżone do *blockchaina* rozważane są przez banki i inne instytucje finansowe jako alternatywa dla istniejących systemów rozliczeniowych. Z kolei banki centralne i krajowi regulatorzy rynku finansowego stają przed wyzwaniami związanymi z emisją przez nadzorowane spółki cyfrowych walut oraz cyfrowych jednostek udziałowych opartych na technologii łańcucha bloków.

Przyjęcie tej technologii przez duże instytucje finansowe może pozostać niezauważalne dla konsumentów, którzy dalej rozliczać się będą w znany im sposób – poszerzeniu ulegać będzie jedynie możliwość korzystania z narzędzi wykorzystujących technologie cyfrowe. Specyfika technologii łańcucha bloków spowoduje jednak, że nawet w takim scenariuszu znacznej modyfikacji będą musiały ulec mechanizmy ochrony konsumentów. Nieodłącznie wpisana w technologię łańcucha bloków decentralizacja utrudni bowiem stwierdzenie, kto z uczestników danej transakcji ponosi odpowiedzialność związaną z jakimś niepowodzeniem lub błędem.

Przykłady dziedzin prawa, które potencjalnie będą musiały zostać zmienione w związku z rozwojem technologii łańcucha bloków, można mnożyć. Być może jednak niemożliwe będzie dokonywanie poszczególnych zmian bez reformy systemu prawa jako całości. Zastosowania *blockchaina* dotykają bowiem najbardziej fundamentalnych instytucji prawnych, takich jak umowy (na temat *smart contracts* pisaliśmy już tutaj) czy osoby prawne (koncepcja *Decentralized Autonomous Organisations*). Na gruncie obowiązujących przepisów takie rozwiązania są bowiem bardzo trudne do wprowadzenia.